Proceedings of the 53rd Hawaii International Conference on System Sciences | 2020

Introduction to the Minitrack on Machine Learning and Cyber Threat Intelligence and Analytics, HICSS 2020

Kim-Kwang Raymond Choo
University of Texas at San Antonio, USA
raymond.choo@fulbrightmail.org

Ali Dehghantanha
University of Guelph, Canada
adehghan@uoguelph.ca

Abstract

One emerging research focus is cyber threat intelligence and analytics, which seeks to integrate and deploy different computing techniques such as big data analytics, sentiment analysis, artificial intelligence (e.g. machine learning) to perceive, reason, learn and defend against advanced cyber attacks or advanced persistent threats, as well as facilitating the collection, preservation and analysis of evidence that may then be used to identify and prosecute the perpetrators. This is the focus of the 'Machine Learning and Cyber Threat Intelligence and Analytics' mini-track, and in this introduction article, we will describe the eight papers accepted in this mini-track.

1. Introduction

With the digitalization of things, significant volume and variety of data are collected from different security monitoring solutions as well as systems that were compromised or have been used to facilitate an attack (e.g. a cloud server, cyber-physical systems, and Internet of Things (IoT) devices including those that are deployed in industrial settings). Thus, advanced cyber threat intelligence and analytical techniques (e.g. threat intelligence, big data and artificial intelligence – broadly defined to include machine and deep learning techniques) are key to real-time detection and mitigation of cyber security incidents, and to the collection and analysis of cyber security incident related information.

The importance of cyber threat intelligence in our digitalized society is partly evidenced by the interest in this mini-track, since it was first included in HICSS 2018 ([1], [2]).

Contributors of the eight accepted papers are from both government agencies and academia, namely: Swedish Defence Research Agency (Sweden), University of Hawaii (United States), University of Nebraska at Omaha (United States), Sam Houston State University (United States), Colorado State University (United States), Stephen F. Austin State University (United States), University of Houston (United States), University of South Alabama (United States). The eight accepted papers are as follows:

1. A Model for Predicting the Likelihood of Successful Exploitation [3]
2. Digit Recognition From Wrist Movements and Security Concerns with Smart Wrist Wearable IOT Devices [4]
3. Knock! Knock! Who is There? Investigating Data Leakage from a Medical Internet of Things Hijacking Attack [5]
4. An Unsupervised Approach to DDoS Attack Detection and Mitigation in Near-Real Time [6]
5. Interpretability of API Call Topic Models: An Exploratory Study [7]
6. Phishing Sites Detection from aWeb Developer's Perspective Using Machine Learning [8]
7. Network Attack Detection using an Unsupervised Machine Learning Algorithm [9]
8. Attack Modeling and Mitigation Strategies for Risk-Based Analysis of Networked Medical Devices [10]

2. Concluding Remarks

In addition to the topics discussed in these eight papers, other topics of relevance to this growing area include:

- Blockchain and its application in cyber security
- Detection and analysis of advanced threat actors tactics, techniques and procedures
- Application of machine and/or deep learning tools and techniques, particularly explainable artificial intelligence (XAI) in cyber threat intelligence
- Theories and models for detection and analysis of advanced persistent threats

URI: https://hdl.handle.net/10125/64530
978-0-9981331-3-3

- Automated and smart tools for collection, preservation and analysis of digital evidences
- Threat intelligence techniques for constructing, detecting, and reacting to advanced intrusion campaigns
- Applying machine and/or deep learning tools and techniques for malware analysis and fighting against cyber crimes
- Intelligent incident response tools, techniques and procedures for contemporary technologies, such as cloud and cyber-physical systems

3. References

[1] Kim-Kwang Raymond Choo and Ali Dehghantanha 2018. Introduction to the Minitrack on Cyber Threat Intelligence and Analytics. In Proceedings of 51st Hawaii International Conference on System Sciences (HICSS 2018). Available on https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1672&context=hicss-51

[2] Kim-Kwang Raymond Choo and Ali Dehghantanha 2019. Introduction to the Minitrack on Cyber Threat Intelligence and Analytics. In Proceedings of 52nd Hawaii International Conference on System Sciences (HICSS 2019). Available on https://scholarspace.manoa.hawaii.edu/handle/10125/60373

[3] Hannes Holm and Ioana Rodhe 2020. A Model for Predicting the Likelihood of Successful Exploitation. In Proceedings of 53rd Hawaii International Conference on System Sciences (HICSS 2020).

[4] Lambert Leong and Sean Wiere 2020. Digit Recognition From Wrist Movements and Security Concerns with Smart Wrist Wearable IOT Devices. In Proceedings of 53rd Hawaii International Conference on System Sciences (HICSS 2020).

[5] Talon Flynn, George Grispos, William Bradley Glisson, and William Mahoney 2020. Knock! Knock! Who is There? Investigating Data Leakage from a Medical Internet of Things Hijacking Attack. In Proceedings of 53rd Hawaii International Conference on System Sciences (HICSS 2020).

[6] Robert McAndrew, Stephen Hayne, and Haonan Wang 2020. An Unsupervised Approach to DDoS Attack Detection and Mitigation in Near-Real Time. In Proceedings of 53rd Hawaii International Conference on System Sciences (HICSS 2020).

[7] Puntitra Glendowne and Dae Glendowne 2020. Interpretability of API Call Topic Models: An Exploratory Study. In Proceedings of 53rd Hawaii International Conference on System Sciences (HICSS 2020).

[8] Xin Zhou and Rakesh M. Verma 2020. Phishing Sites Detection from aWeb Developer's Perspective Using Machine Learning. In Proceedings of 53rd Hawaii International Conference on System Sciences (HICSS 2020).

[9] Avinash Kumar, William Bradley Glisson, and Ryan Benton 2020. Network Attack Detection using an Unsupervised Machine Learning Algorithm. In Proceedings of 53rd Hawaii International Conference on System Sciences (HICSS 2020).

[10] Bronwyn J. Hodges, J. Todd McDonald, William Bradley Glisson, Michael Jacobs, Maureen Van Devender, and J. Harold Pardue 2020. Attack Modeling and Mitigation Strategies for Risk-Based Analysis of Networked Medical Devices. In Proceedings of 53rd Hawaii International Conference on System Sciences (HICSS 2020).